REMARKS

Claims 1-12 are pending in this application with claims 1 and 9 being amended by this response.

Claims 1 and 9 have been amended for clarity in response to the comments made by the Examiner.

Objection to the Specification

The specification is objected to as not placing the headings in proper position. The specification has been amended in accordance with the comments of the Examiner to correct a typographical error in the previous response and place the cited headings in their proper positions. In view of the amendments to the specification, it is respectfully submitted that this objection is satisfied and should be withdrawn.

Rejection of Claims 1-6, 8 and 10-12 under 35 USC § 103(a)

Claims 1-6, 8 and 10-12 is rejected under 35 U.S.C. 103(a) as being anticipated by Linnartz (U.S. Patent No. 6,314,518 B1) in view of Cooperman et al. (U.S. Patent No. 5,613,004).

The present invention as claimed in claim 1 describes a method of protection against the copying of digital data stored on an information carrier. A permission or a prohibition to copy and/or to play digital data is delivered as a function of the identification or otherwise of at least an encryption of the digital data and a watermarking of the digital data.

Linnartz discloses a system for copy protecting content information stored on a record carrier. The content, for example an MPEG digital video stream, is watermarked and includes a control signal indicating the status. In the receiver device, a check is performed to allow playback depending on the watermark. The playback device checks

the watermark information against further supplemental information, such as a physical mark on the record carrier or the control signal.

Linnartz describes a system wherein the detection of the watermark in the MPEG video stream takes place outside the drive in an external MPEG decoder and the detected watermark information is transmitted to the drive, which performs the playback control. In order to secure the link between the drive unit and the MPEG decoder, an encryption/decryption of the data is performed to create a secure path between both devices. Although Linnartz describes encrypting data circulating on a link between a drive device which receives data from a record carrier and controls the playback of the data and an MPEG decoder which performs watermark detection, Linnartz, as admitted in the Office Action, neither discloses nor suggests "delivering a permission or a prohibition to copy and/or to play said digital data as a function of the identification or otherwise of at least and encryption of said digital data; and a watermarking of said digital data," as recited in claim 1 of the present invention.

Cooperman et al. describe a method and apparatus for encoding and decoding additional information into a stream of digitized samples in an integral manner. The information is encoded using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The method makes it extremely difficult to find the information in the samples if the proper keys are not possessed by the decoder.

Cooperman et al. disclose in the "Background of the Invention" that "three general types of schemes have been implemented in an attempt to protect copyrights" (Col. 2, lines 27-31) of digitized data:

1) Encryption (or scrambling) of the data (see col. 2, lines 36-56);
2) "Copy Protection" which Cooperman et al. describe as a "various method by which a software engineer can write the software in a clever manner to determine if it has been copied, and if so to deactivate itself...[and] undocumented changes to the storage format of the content" (Col. 2, lines 57-67); and

3) "Content Extension" which Cooperman et al. describe as adding extra information to the original data. This information indicates whether the data can be copied or not (see col. 3, lines 1-12).

The Office Action asserts that Cooperman et al. disclose a digital data protection method that uses encryption of the digital data and a watermarking of the digital data. Cooperman et al. are concerned with improving on the above methods by combining "steganography-obscuring information that is otherwise in plain sight, and cryptography-scrambling information" (Col. 3, lines 50-51). However, unlike the present claimed invention, Cooperman et al. do not use cryptography to **encrypt the content** itself. Rather, Cooperman et al. use cryptography to **encrypt the message that is hidden** in the original content and use keys to locate the hidden message within the content (see col. 3, lines 28-45).

The passages cited by the Office Action (col. 3, lines 48-52 and col. 5, lines 30-47) present the invention of Cooperman et al., in a general manner, as combining two techniques: steganography and cryptography. The passages then present the technique of Cooperman et al. (in col. 5, lines 30-47) in a more detailed manner. According to this technique, specific information **about the content** (to uniquely identify the content and/or the content owner and/or a licensed publisher or subscriber...) is **inserted** in a certificate which is **encrypted** and **inserted in a hidden manner** (i.e. as a watermark) in the original content. This watermark can only be recovered with specific "masks" or keys available only to authorized parties. Therefore, Cooperman et al., similarly to Linnartz, neither disclose nor suggest "delivering a permission or a prohibition to copy and/or to play said digital data as a **function of the identification or otherwise** of at least and encryption of said digital data and a watermarking of said digital data," as recited in claim 1 of the present invention.

Furthermore, the Office Action asserts that it would have been obvious to modify Linnartz's method in light of the teachings of Cooperman et al. to disclose the features of claim 1 of the present invention. However, Cooperman et al., as discussed above, merely disclose separately encrypting and watermarking additional digital data

(which itself is well known). Therefore, it is respectfully submitted that the combined system, similarly to the individual systems of Linnartz and Cooperman et al., neither disclose nor suggest "delivering a permission or a prohibition to copy and/or to play digital data stored on an information carrier as a function of the identification or not of an encryption of said digital data and a watermarking of said digital data" as recited in claim 1 of the present invention.

Furthermore, the method of the present claimed invention allows determination of whether digital data may be copied (or played back) or not on the basis of the detection of an encryption of the data **and** a watermarking of the data. This is unlike Cooperman et al. which add extra information ("Content Extensions") in the data. Additionally, the watermark that is detected in the data in the present claimed invention need not have a payload (i.e. it carries no specific information). It is only the presence or absence of a watermark that determines (in combination with the identification of an encryption or not of the data) a permission or prohibition to copy and/or to play the data. Therefore, it is respectfully submitted that the combined system, similarly to the individual systems of Linnartz and Cooperman et al., neither disclose nor suggest "delivering a permission or a prohibition to copy and/or to play digital data stored on an information carrier as a function of the identification or not of an encryption of said digital data and a watermarking of said digital data" as recited in claim 1 of the present invention.

As claims 2-6, 8 and 10-12 are dependant on independent claim 1, it is respectfully submitted that they are allowable for the same reasons as discussed above in regards to claim 1. In view of the above remarks and amendments to the claims it is respectfully submitted that there is no 35 USC 112 compliant enabling disclosure in Linnartz and Cooperman et al., when taken alone or in combination, showing the above discussed features. It is thus, further respectfully submitted that this rejection is satisfied and should be withdrawn.

Rejection of Claim 7 under 35 USC § 103(a)

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz (U.S. Patent No. 6,314,518 B1) in view of Cooperman et al. (U.S. Patent No. 5,613,004) and further in view of Ichinoi (U.S. Patent No. 6,266,477).

Ichinoi describe a data signal recording and playback method and apparatus that determines whether the recording medium being used is a high-performance recording medium for recording and playing back both digital and analog signals, or a standard performance medium, and selecting its recording specifications accordingly.

The Office Action asserts the Ichinoi discloses a conversion of the digital data into analog signal and a corruption of the analog signal if a prohibition of digital copying is delivered. However, Ichinoi, similarly to Linnartz and Cooperman et al., neither discloses nor suggests "delivering a permission or a prohibition to copy and/or to play said digital data as a function of the identification or otherwise of at least and encryption of said digital data and a watermarking of said digital data," as recited in claim 1 of the present invention.

Furthermore, the Office Action asserts that it would have been obvious to combine the teaching of Ichinoi to the systems of Linnartz and Cooperman et al. However, the combined system, similarly to the individual systems of Ichinoi, Linnartz and Cooperman et al., would neither disclose nor suggest "delivering a permission or a prohibition to copy and/or to play said digital data as a function of the identification or otherwise of at least and encryption of said digital data and a watermarking of said digital data," as recited in claim 1 of the present invention.

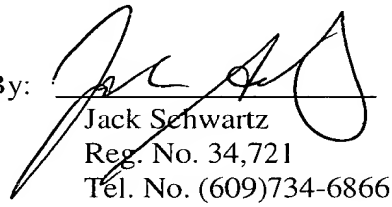
As claim 7 is dependent on claim 1, it is respectfully submitted that it is allowable for the same reason as discussed above in regards to claim 1. In view of the above remarks and amendments to the claims it is respectfully submitted that there is no 35 USC 112 compliant enabling disclosure in Linnartz, Cooperman et al. and

Ichinoi, when taken alone or in combination, showing the above discussed features. Thus, applicant respectfully submits that Linnartz, Cooperman et al. and Ichinoi, when taken alone or in combination, fail to disclose all the features of claim 7. It is thus, further respectfully submitted that this rejection is satisfied and should be withdrawn.

Having fully addressed the Examiner's rejections, it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at the phone number below, so that a mutually convenient date and time for a telephonic interview may be scheduled.

No additional fee is believed due. However, if an additional fee is due, please charge the additional fee to Deposit Account 07-0832.

Respectfully submitted,
Sylvain Chevreau et al.

By: 
Jack Schwartz
Reg. No. 34,721
Tel. No. (609)734-6866

Thomson Licensing Inc.
Patent Operations
PO Box 5312
Princeton, NJ 08543-5312
August 30,2005

CERTIFICATE OF MAILING under 37 C.F.R. §1.8

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

Date: August 30, 2005 Karen Schwarch